Amendments to the Drawings:

The attached sheet of drawings includes a replacement drawing sheet, replacing the previously added replacement sheets, including 2nd, 3rd, and 4th drawing sheets. The attached sheet is a replacement drawing attached hereto replaces the objected-to replacement drawings submitted on December 14, 2004, illustrating alternative embodiments previously described.

Attachment: Replacement sheet for the drawing sheets 2 through 4.

Remarks:

This paper is in response to the final office action dated March 18, 2005 with respect to Application No. 09/646,640. Claims 2-13 stand rejected. Applicant cancels claims 2-9, amends Claim 10 and adds Claims 14 and 15. Claims 10-15 are pending in the Application. Claims 2-7 stand rejected under 35 U.S.C. 112, second paragraph as being indefinite. Claims 2-7 have been canceled. Claims 2-13 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier Applied Cryptography (hereinafter referred to as "Schneier") in view of Kocher "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS and Other Systems" (hereinafter referred to as "Kocher").

Claims 14 and 15 have been added. Support for new Claim 14 is found on pages 5 and 6 of the translated specification. Support for new Claim 15 is found in the originally presented claims. No new matter is presented thereby.

New drawings 2-4 are filed herewith to replace drawings filed on December 14, 2004. The new drawings address the objections to the drawings filed on December 14, 2004 and follow the suggestion provided in paragraph 9 of the Office Action.

Applicant acknowledges the withdrawal of the objection to the title and appreciates the withdrawal.

Applicant traverses the rejections applicable to the remaining claims and respectfully requests withdrawal of any rejection and an indication of allowance for the reasons set forth below.

Rejection under 35 U.S.C. 103(a) Schneier in view of Kocher

As described in the specification, the claims are directed to solving a current problem in the state of the art concerning measurement of power consumption of an electronic device (by means of an oscilloscope) and observing its behavior. For example, a power trace of the device that performs an encryption using the DES algorithm. The

power consumption is not constant and reveals some patterns. Knowing that DES takes typically 16 rounds to encrypt the input data it is possible to identify the rounds in the 16 repeating patterns in the power trace. Although this is an interesting observation it does not give an answer to the more important question: what is the key used for this encryption? Hackers proposed Differential Power Analysis (DPA) to retrieve the key of a cryptographic algorithm by analyzing several of measured power traces. An attacker only needs to know either the clear text (input) or cipher test (output) of the algorithm. The basic idea behind the attack is the assumption that there is a correlation between data values being processed by the device and the power consumption. In other words and for explanation purposes: it is conceptually assumed that processing a bit value zero uses less energy than processing a bit value one (or vice versa).

By using different input values it results in a small difference in power consumption and a key can be identified by inspection of differential traces. By computing differential traces it is possible to "identify" the clock cycles where input data is being processed. Moreover, by considering all input bits to a cryptographic algorithm and creation of differential traces for each pair (a trace for a bit value zero and a trace for a bit value one), it is possible to identify the exact timing of their appearance in the program code. In situations where noise prevents the recognition of peaks in the differential trace it is possible to increase the number of samples and compute a differential trace out of many individual traces.

Claim 10 provides for "randomly modifying the order of execution of operations from one cycle to another" making the differential analysis between races is made difficult or even impossible because processing orders are modified.

Applicant has amended Claim 10 to address the rejection provided in the final office action. More particularly, amended Claim 10 provides a "Data protection method, for protecting data elements processed by a microprocessor in a chip card from discovery by analysis of the microprocessor's electric power consumption said method using a

cryptographic algorithm for executing operations for processing said data elements so as to generate encrypted information, said method comprising: randomly modifying the order of execution of operations from one cycle to another, a cycle being a complete execution cycle of the algorithm or an intermediate cycle of a group of operations, said operations being operations whose order of execution relative to the others does not affect the result, thereby protecting said data elements processed by a microprocessor in a chip card from discovery by analysis of the microprocessor's electric power consumption."

Neither Schneier nor Kocher, neither alone nor in combination, teach the elements of Claim 10 and, specifically protecting data elements from discovery by analysis of a microprocessor's electric power consumption. Schneier, as stated in paragraph 21 of the final office action, does not expressly disclose incorporating a data protecting method to protect data elements from discovery by analysis of a microprocessor electric power consumption. Likewise, Kocher fails to teach incorporating a data protecting method to protect data elements from discovery by analysis of a microprocessor electric power consumption as claimed in Claim 10. Kocher teaches a method of using a blinding factor to mask a data element in a cryptographic method. Although paragraph 21 states that timing attacks observing different amounts of time to process different inputs inherently includes different power fluctuations generated by the different amounts of time, Applicant respectfully disagrees and points out that a blinding factor to mask a data element would, in fact, highlight the data element. In fact, the method described on page 1 of the specification would assist an attacking in locating such a mask: "variations in the electromagnetic radiation such that the envelope of electromagnetic radiation is indicative of the data processed." By masking a data element, the envelope described in the specification would, in fact, highlight the locations of a data element mask and help an attacker locate such a mask and the hidden data. Moreover, masking a data element as described in Kocher would teach away from the elements of Claims 10 because a mask would be inappropriate for a "chip card" as claimed. A chip card requires an algorithm that can be executed quickly, teaching away from a "mask" type cryptographic method. Thus, the

combination of Schneier and Kocher fail to teach the elements of Claim 10. Furthermore, contrary to MPEP § 2143.01, there is no suggestion or motivation to combine the teachings of Schneier and Kocher. Neither Schneier nor Kocher address issues addressed and solved in the elements of Claim 10. Thus, for this reason and for the failure of the combination to each the elements of Claim 10, the combination is not only prohibited, but fails to teach the elements of Claim10.

Applicant further respectfully points out that neither Kocher nor Schneier, either alone or in combination, teach a "data protection method using a cryptographic algorithm for executing operations for processing data elements so as to generate encrypted information, said method comprising randomly modifying the order of execution of operations from one cycle to another, a cycle being a complete execution cycle of the algorithm or an intermediate cycle of a group of operations, said operations being operations whose order of execution relative to the others does not affect the result." The final office action in paragraph 22 describes DES cryptographic methods as having a subset of consecutive operations that are commutative. The commutative nature of such operations, according to paragraph 22, allows for inverse transformation without changing the encrypted information. Paragraph 26 of the final office action provides that the commutative property of many of the steps within a cycle in DES trivially allows for reordering operations without changing the resulting encrypted text. Applicant respectfully disagrees that the use of the commutative property in DES teaches the element of "randomly modifying the order of execution of operations from one cycle to another, a cycle being a complete execution cycle of the algorithm or an intermediate cycle of a group of operations, said operations being operations whose order of execution relative to the others does not affect the result" as claimed. Specifically, the inherent properties of DES do not teach "randomly modifying the order of execution of operations from one cycle to another" as claimed. Randomly modifying the order of execution of operations from one cycle to another is an unobvious difference from using the commutative properties of DES. Moreover, the teachings of Schneier in combination with Kocher do not teach "randomly modifying the order of execution of operations from one cycle to another" as claimed,

either alone or in combination. Additionally, paragraph 26 of the final office action cites MPEP 2112(1) for the proposition that something old "randomly modifying order of execution of commutative operations" does not become patentable upon the discovery of a new property. Applicant respectfully points out that the claim elements do not state "randomly modifying order of execution of commutative operations" and thus the "old" described in the final office action does not describe Claim 10. DES does not address modifying the order of execution of operations "from one cycle to another" as claimed. Importantly, the commutative property does not address timing of any modification of any operation. Rather, the elements as claimed, the random modification of the order of execution of operations from one cycle to another prevents hackers from being able to perform differential analysis between traces detected from signals emitted from a chip card. Thus, contrary to paragraph 26, the Applicant has not discovered "a previously unappreciated property of a prior art composition, or of a scientific explanation for the prior art's functioning" as described in Atlas Powder Co. v. Ireco Inc., 190 F.3d 1342, 1347, 51 USPQ2d 1943, 1947 (Fed. Cir. 1999).

For the reasons provided above, neither Schneier nor Kocher, either alone or in combination teaches the elements of Claim 10, and Claim 10 is allowable. Claims 11-13 depend from Claim 10 are allowable with Claim 10.

Claim Objections

Examiner objected to claim 9 due to misspelling. Applicant cancels claim 9 herein thus making the objection moot.

The application is now deemed to be in condition for allowance and notice to that effect is solicited.

CONCLUSION

It is submitted that all of the claims now in the application are allowable. Applicants respectfully request consideration of the application and claims and its early allowance. If the Examiner believes that the prosecution of the application would be facilitated by a telephonic interview, Applicants invite the Examiner to contact the undersigned at the number given below.

Applicants respectfully request that a timely Notice of Allowance be issued in this application.

Respectfully submitted,

Date: Aug 18, 2005

Pehr Jansson
Registration No. 35,759

Attn: Pehr Jansson
7628 Parkview Circle
Austin, TX 78731-1127
512-241-0837
678-868-0101 (Fax)
pehr@pehrjansson.com